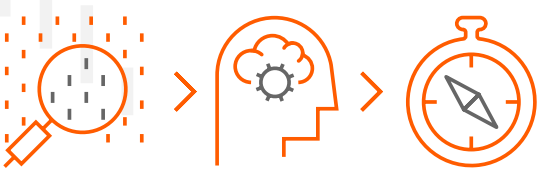
SonicWall Analytics

Trasforma i dati in informazioni immediatamente fruibili

SonicWall Analytics trasforma i dati di traffico dei firewall in informazioni concrete sugli utenti, le applicazioni e le reti, permettendo di limitare i rischi di sicurezza con maggiore precisione e velocità. Il tutto da un'unica interfaccia. Basato su un'architettura ad alte prestazioni, il motore di analisi elabora un'enorme quantità di dati grezzi provenienti da migliaia di nodi firewall su larga scala per offrire la massima trasparenza e visibilità della sicurezza attraverso un pannello di controllo.

Analytics crea rappresentazioni visive delle conoscenze dei set di dati utilizzando varie forme di grafici semantici, diagrammi di tempo/utilizzo e tabelle per ridurre i silos di dati e facilitare il lavoro degli analisti. Le funzionalità di drill-down aggiuntive consentono ai responsabili della sicurezza di analizzare ed eliminare punti di dati critici per **intervenire tempestivamente sui rischi nascosti** e adottare policy basate sull'evidenza contro attività rischiose degli utenti man mano che procedono nel processo di rilevamento.

Grazie alla visibilità e al controllo completi, gli analisti di sicurezza possono vedere ogni cosa ovunque e gestire meglio il rischio, mentre gli addetti alla gestione degli incidenti possono concentrarsi sulla pianificazione di azioni di risposta rapida per le applicazioni e gli utenti più importanti, senza dover reagire a ogni evento. Analytics è scalabile e offre **agilità ed elasticità nel cloud** per soddisfare i più complessi requisiti aziendali.



CARATTERISTICHE PRINCIPALI

Business

- Massima trasparenza sulla sicurezza
- Istantanee in tempo reale sul livello di sicurezza
- Rispetto delle normative di conformità interne
- Pianificazione e creazione di budget accurati per la cybersicurezza
- Riduzione di CAPEX e OPEX

Operatività

- Comprensione immediata dei dati di sicurezza
- Informazioni su ogni attività di rete e degli utenti con relativi avvisi
- Creazione di policy di difesa accurate
- Scalabilità e performance per la massima agilità nel cloud

Sicurezza

- Rilevamento dei rischi nascosti
- Capacità di intervento precoce
- Reazione tempestiva alle attività non sicure degli utenti
- Aiuta gli analisti a gestire meglio il rischio
- Semplifica la risoluzione dei problemi

Maggiori informazioni su SonicWall Analytics

www.sonicwall.com/analytics

SCHEDA TECNICA

Vedere ogni cosa ovunque

Analytics offre una visione completa dell'intero ambiente di sicurezza SonicWall a livello di tenant, gruppi o dispositivi. Il pannello di controllo offre l'analisi e il monitoraggio statici in tempo quasi reale di tutto il traffico di rete e delle comunicazioni di dati che attraversano l'ecosistema dei firewall. Tutti i dati di log vengono registrati, aggregati, contestualizzati e presentati in un modo significativo e facilmente fruibile che permette di scoprire, interpretare e valutare i dati per adottare le necessarie misure di difesa in base a informazioni basate sui dati.

Figura 1.0 Pannello di controllo

Analytics offre un'ampia gamma di report predefiniti, che possono essere inviati a richiesta o su base regolare. Offre inoltre la flessibilità di creare report personalizzati con metriche e valori scelti da un'ampia libreria di tipi di dati firewall, permettendo di assemblare ed estrarre in modo logico informazioni preziose da dispositivi specifici di determinati gruppi o tenant. I report personalizzati aiutano a interpretare i dati, offrendo ai responsabili delle decisioni e agli addetti alla sicurezza una maggiore visibilità e informazioni pratiche da set di dati più piccoli ma di maggiore qualità per l'analisi del traffico e la ricerca di anomalie e falle di sicurezza. In questo modo è possibile esaminare l'analisi corretta, prendere decisioni informate e attuare tempestivamente le policy necessarie in base a dati affidabili.

Comprendere l'esposizione al rischio

Le funzioni di drill-down e pivoting consentono di esaminare in dettaglio modelli specifici e tendenze relative al traffico in entrata/in uscita, all'uso delle applicazioni, all'accesso di utenti e dispositivi, alle minacce e molto altro ancora. Mediante una combinazione di report e analisi su endpoint, reti, utenti e applicazioni è possibile analizzare o reagire proattivamente ad avvisi, anomalie e attività rischiose degli utenti. La massima trasparenza della sicurezza migliora la consapevolezza della situazione e permette di rilevare i rischi di sicurezza, coordinare le policy, applicare misure di sicurezza coerenti e monitorare costantemente i risultati nel proprio ambiente.

Ottimizzare la produttività della forza lavoro

User Analytics offre una visione ampia e trasparente delle applicazioni Web e delle attività di utilizzo di Internet della forza lavoro. Le funzionalità di drill-down consentono agli analisti di esaminare e analizzare i dati interessati e di stabilire misure basate su policy comprovate per utenti e applicazioni rischiose nel momento in cui vengono rilevate. Inoltre, Productivity Reports fornisce informazioni sull'utilizzo di Internet e sul comportamento dei dipendenti in un periodo specificato. Genera istantanee accurate e report dettagliati che classificano le attività Web degli utenti per gruppi di produttività come ad esempio gruppi produttivi, non produttivi, accettabili, non accettabili o definiti dall'utente, aiutando le organizzazioni a comprendere e controllare meglio l'utilizzo di Internet.

Implementazione flessibile con servizi SaaS, virtuali o IaaS

Analytics offre opzioni d'installazione flessibili per soddisfare al meglio i diversi requisiti operativi.

Analytics è integrato nel servizio Network Security Manager (NSM) SaaS gestito in hosting da SonicWall, accessibile tramite Internet e senza bisogno di manutenzione. L'opzione SaaS offre una flessibilità illimitata con scalabilità on-demand, riducendo allo stesso tempo i costi operativi. I tipici costi per l'acquisto di hardware e software, l'installazione personalizzata, la manutenzione ordinaria, gli aggiornamenti, l'ammortamento degli asset e il ritiro dei prodotti vengono sostituiti da un costo annuale di abbonamento contenuto e prevedibile.

Per il controllo e la conformità completi del sistema è possibile installare la versione software di Analytics in azienda su una piattaforma virtuale a scelta, come VMware. In questo modo si ottengono tutti i vantaggi operativi ed economici della virtualizzazione, come scalabilità del sistema, velocità di provisioning e riduzione dei costi.

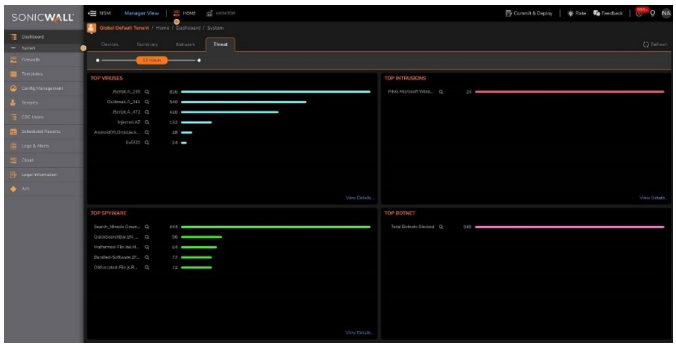


Figura 2.0 Riepilogo delle minacce

Riepilogo delle funzionalità

Funzionalità	Descrizione
Analisi degli utenti	Mostra una panoramica completa delle attività in rete della forza lavoro, delle applicazioni e delle potenziali minacce tramite una dashboard interattiva. Consente un'analisi granulare dei dati storici per stabilire misure basate su dati concreti contro le attività rischiose degli utenti nel web.
Analisi del traffico delle applicazioni	Offre alle aziende informazioni dettagliate sul traffico delle applicazioni, sull'uso della larghezza di banda e sulle minacce alla sicurezza, oltre a potenti funzioni di risoluzione dei problemi e analisi forense.
Analisi della sicurezza	Visibilità in tempo reale e rapido rilevamento delle minacce. Consente agli analisti di sicurezza e agli addetti alla gestione degli incidenti di cercare, identificare e analizzare i problemi.
Visualizzazione dinamica in tempo reale	Mediante un unico pannello di controllo, gli analisti della sicurezza possono eseguire approfondite analisi investigative e forensi dei dati di sicurezza con maggiore precisione, chiarezza e velocità.
Rapido rilevamento e correzione	Le funzionalità investigative consentono di monitorare le attività non sicure e di gestire ed eliminare rapidamente i rischi con misure adeguate.
Report sulla produttività	Forniscono informazioni dettagliate sull'uso delle risorse Internet in tutta l'organizzazione e consentono di generare potenti snapshot e report dettagliati sul comportamento di accesso a Internet degli utenti.

Funzionalità	Descrizione
Report personalizzati	Workflow autoguidato per creare report personalizzati con metriche e valori scelti da un'ampia libreria di tipi di dati firewall.
Report a livello di tenant e gruppi	Gli utenti possono visualizzare report predefiniti o personalizzati a livello del gruppo di dispositivi o del tenant.
Report VPN	Forniscono un riepilogo delle risorse aziendali utilizzate nel tunnel VPN, della larghezza di banda consumata e degli utenti responsabili (nome utente e indirizzo IP). Gli amministratori di rete possono usare queste informazioni per monitorare le applicazioni business-critical, controllare o strutturare il traffico e pianificare un incremento della capacità.
Analisi e rapporti sui flussi	Monitoraggio in tempo reale e cronologico, grazie all'agente di reporting del flusso per l'analisi del traffico delle applicazioni e ai dati di utilizzo tramite i protocolli IPFIX o NetFlow. Un'interfaccia intuitiva ed efficace consente agli amministratori di monitorare visivamente la propria rete in tempo reale, con la capacità di individuare le applicazioni e i siti web che richiedono più larghezza di banda, visualizzare l'uso delle applicazioni per ogni utente e anticipare le minacce e gli attacchi diretti alla rete. • Schermata con report in tempo reale e filtraggio con un semplice clic • Dashboard sui flussi principali con pulsanti per la visualizzazione in base a categorie • Schermata con rapporti sui flussi, con schede aggiuntive sugli attributi dei flussi • Schermata di analisi dei flussi con potenti funzioni di correlazione e pivoting • Visualizzatore di sessioni per analisi drill-down approfondite di singole sessioni e pacchetti
Report grafici dettagliati	Forniscono visibilità su attacchi ai firewall, uso della larghezza di banda, produttività dei dipendenti, attività sospette in rete e analisi del traffico delle applicazioni.
Report basati su syslog (solo per Analytics 2.5)	Semplificano il riepilogo dei dati, offrendo report quasi in tempo reale sui messaggi syslog in arrivo. L'accesso diretto ai dati grezzi sottostanti garantisce una migliore granularità delle analisi e la personalizzazione dei report.
Report pianificati	Forniscono un unico modello base per tutti i report pianificati. Un report può combinare diagrammi e tabelle per diverse unità. I report possono essere pianificati e inviati in diversi formati a uno o più analisti.
Report immediati	Viste personalizzabili per visualizzare diversi report di riepilogo in un'unica pagina. Gli utenti possono consultare facilmente dati essenziali della rete e analizzare in poco tempo le informazioni contenute in svariati report.
Report dettagliati sulle minacce	Raccolgono informazioni sugli attacchi e forniscono l'accesso immediato alle attività delle minacce rilevate dai firewall SonicWall mediante i servizi di gateway anti-virus, anti-spyware, prevenzione delle intrusioni, controllo e intelligence delle applicazioni.
Nuova intelligence degli attacchi	Fornisce report granulari su determinati tipi di attacco o tentativi d'intrusione e sull'indirizzo di origine dell'attacco, per poter reagire rapidamente alle minacce ricorrenti.
Report su punti di accesso wireless non autorizzati	Mostrano tutti i dispositivi wireless in uso e i comportamenti non autorizzati da connessioni di rete ad hoc o peer-to-peer tra gli host e associazioni accidentali per gli utenti che si collegano a reti vicine non autorizzate.
Report di Capture ATP	Dashboard intuitiva per l'analisi delle minacce e report con risultati dettagliati dell'analisi per i file che sono stati inviati al servizio, con informazioni come sorgente e destinazione, e un riepilogo accurato della reazione del malware dopo la detonazione.
Report Botnet	Sono disponibili quattro tipi di report (tentativi, obiettivi, iniziatori e cronologia), contenenti informazioni di contesto sui vettori di attacco come ID delle botnet, indirizzi IP, paesi, host, porte, interfacce, iniziatore/obiettivo, origine/destinazione e utente.
Report GeoIP	Contengono informazioni sul traffico bloccato in base al Paese di origine o di destinazione del traffico. Sono disponibili quattro tipi di rapporti (tentativi, obiettivi, iniziatori e cronologia), contenenti informazioni di contesto sui vettori di attacco come ID delle botnet, indirizzi IP, paesi, host, porte, interfacce, iniziatore/obiettivo, origine/destinazione e utente.
Sistema di logging centralizzato	Un unico strumento centralizzato per consolidare gli eventi di sicurezza e i log di tutti gli apparati gestiti o per effettuare analisi forensi della rete.
Architettura cloud-native	Consente di raccogliere, combinare, elaborare, riprocessare, estrarre, correlare e caricare enormi quantità di dati da decine di migliaia di nodi firewall, sfruttando la velocità e l'elasticità del cloud.

Licenze e pacchetti

Reporting				
Funzionalità	SaaS Analytics per NSM Essential	SaaS Analytics per NSM Advanced	Analytics on-premise	Analytics on-premise
Registro dei log	Basato su Netflow/ IPFIX[1]	Basato su Netflow/ IPFIX[1]	Basato su Netflow/ IPFIX[1]	Basato su syslog[1]
Dashboard a livello di gruppo/tenant	Sì	Sì	No	No
Capture ATP (a livello di dispositivo)	Sì	Sì	Sì	Sì
Capture Threat Assessment (CTA) - a livello di dispositivo	Sì	Sì	Sì	No
Report sulla produttività[3]	No	Sì	No	No
Report VPN	No	Sì	No	Sì
Report personalizzati	No	Sì	Sì	Sì
Report pianificati (flusso, syslog, CTA o gestione)	Sì (tranne flusso)	Sì	Sì	Sì
Giorni di report dei dati	7 giorni	365 giorni	365 giorni	365 giorni
Analisi				
Giorni di analisi dei dati	-	30 giorni	90 giorni	90 giorni
Analisi basate sull'utente	No	Sì	Sì	Sì
Analisi delle applicazioni	No	Sì	Sì	Sì
Analisi forensi della rete e ricerca minacce con drill-down e pivoting	No	Sì	Sì	Sì
Supporto tecnico	Supporto 24x7	Supporto 24x7	Supporto 24x7[2]	Supporto 24x7[2]

[1] Richiede il servizio AGSS/CGSS o un servizio Capture Security Center a pagamento
[2] Richiede una licenza di supporto 24x7
[3] Richiede la licenza AGSS/CGSS attivata sui firewall di generazione 6/6.5, la licenza Essential Protection sui firewall di generazione 7

Requisiti minimi di sistema

Per SonicWall Analytics in modalità SaaS tramite Network Security Manager:

Appliance SonicWall supportate:

- Appliance di sicurezza di rete SonicWall: serie NSA, serie NS*a*, appliance della serie TZ, SOHO-W, SOHO 250, SOHO 250W
- Appliance di sicurezza di rete SonicWall virtuali: da NS*v* 10 a NS*v* 400

Firmware SonicWall supportato

- SonicWall SonicOS 6.0 o superiore

Browser

- Microsoft® Internet Explorer 11.0 o superiore (non usare la modalità di compatibilità)
- Mozilla Firefox 37.0 o superiore
- Google Chrome 42.0 o superiore
  Safari (versione più recente)

Per l'installazione on-premise di SonicWall Analytics:

Appliance virtuale

- Hypervisor: VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V Win 2016
- RAM consigliata: illimitata (minimo 8 GB)
- Hard disk: Base OVA 65 GB con montaggio esterno
- vCPU: 4/illimitate
- Interfaccia di rete: 1
- Guida alla compatibilità VMware

Firmware SonicWall supportato

- SonicWall SonicOS 6.0 o superiore

Appliance SonicWall supportate:

- Appliance di sicurezza di rete SonicWall: serie NS*sp*, SuperMassive E10000 e 9000, serie NSA, serie NS*a*, appliance della serie TZ, SOHO-W, SOHO 250, SOHO 250W
- Appliance di sicurezza di rete SonicWall virtuali: serie NS*v*

Maggiori informazioni su SonicWall Analytics

www.sonicwall.com/analytics

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative per la nuova normalità iperdistribuita, in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibili economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni visitare www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

Datasheet-Analytics-A4-JK-8806